Towards Location- and Orientation-Independent RFID Authentication with COTS Devices

Yinan Zhu*, Chunhui Duan†, Xuan Ding*
*School of Software and BNRist, Tsinghua University, China
†School of Computer Science and Technology, Beijing Institute of Technology, China
Email: yn-zhu19@mails.tsinghua.edu.cn, duanch@bit.edu.cn, dingxuan@tsinghua.edu.cn

***Abstract*—To authenticate tags against counterfeiting, RF fingerprinting technique is widely exploited. However, the status of tagged item is always changed by movement, rotation and other operations. When the item's location or orientation changes, the capability of past methods would be severely affected and their supported authentication ranges are fairly small. To overcome this challenge, we propose the first-of-its-kind method *FreeAuth* to achieve certain location- and orientation-independent RFID authentication without any customized devices, by attaching a tag-pair and hopping the frequency channels and transmission powers. The key insight of *FreeAuth* lies in an implicit fingerprint matching scheme where the distance-frequency-power and orientation-frequency-power relationships are leveraged to circumvent these two negative factors. We implement a prototype of FreeAuth with COTS devices and the experiments demonstrate that FreeAuth is able to achieve around 0.8m and 0.6m ranges along 2D axes, in which the authentication accuracy is over 80%. The average effective authentication range of FreeAuth can outperform the state-of-the-art method by 11.67×.**

***Index Terms*—RFID authentication, Robustness, Effective authentication range, Frequencies and powers hopping**

I. Introduction

With the wide adoption of RFID techniques to label items, the counterfeiting problems of RFID tags have drawn increasing attention, which the cryptographic methods fail to address since commodity tags are battery-free and have little computational capability. To defend against counterfeiting, past works focus on *hardware fingerprint*-based methods and numerous kinds of fingerprints are proposed to authenticate the tags [1]–[7].

Nevertheless, most of these fingerprints need dedicated devices such as software defined radios to obtain [2], [3], [8]–[10], and the rest using commercial off-the-shelf (COTS) devices have very low robustness to dynamic indoor environments or tags' own state changes (*e.g.*, movement, rotation). This is because the fingerprints are extracted from tags' backscatter signals and the signal features are easily affected by environmental factors [11], [12]. The problem of *robustness* limits the practical utility of past schemes since the environment during fingerprint registration and authentication may be entirely different. For example, the locations and orientations of the tagged items are impossible to remain unchanged all the time. Hence, how to robustly authenticate the tags with only COTS devices is still a critical and unsolved problem.

Fig. 1: Experimental setup of FreeAuth

TABLE I: Comparison of FreeAuth with the related methods.

Method	Rotation	Movement	Accuracy in the 0.5m×0.5m region
TagPrint [4]	✗	✗	< 20%
RF-Mehndi [5]	✗	✗	< 30%
EingerPrint [6]	✓	✗	< 75%
FreeAuth	✓	✓	**82.35%∼89.87%**

In this paper, we propose *FreeAuth* that can precisely authenticate RFID tags, regardless of orientation changes or location changes within a certain range. FreeAuth requires only one COTS reader and a single antenna, with high ubiquity and little overhead. In the FreeAuth, we first employ a tag-pair for each item identification, choose the coupling-based phase noise as fingerprint, and then innovatively exploit the relationships of distance-frequency-power and orientation-frequency-power behind the phase offset matrix for implicit fingerprint matching. The essential insights of FreeAuth are twofold. On one hand, through various reader configurations (*e.g.*, channel hopping), we can enlarge the hardware diversity of tag-pair's inductive coupling. On the other hand, the implicit matching algorithm is beneficial to robustness enhancement by circumventing the effects of distance and orientation. In this way, the authentication accuracy of FreeAuth can maintain at a relatively high level as compared to the state-of-the-art (SOTA) methods (see Table I), even when the item rotates to other angles or moves to other positions in a certain range.

II. System Design

As shown in Fig. 2, our system for fingerprint validation contains three parts: 1) phase matrix preprocessing; 2) fingerprint matching; 3) tagged item validation. Below we introduce the workflow.

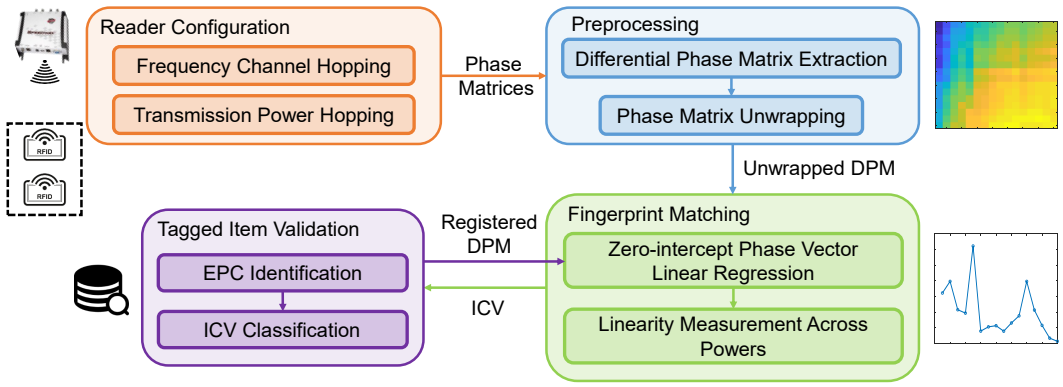


Fig. 2: System overview of FreeAuth

Phase matrix preprocessing. After collecting the backscatter signal features from tag-pair under different frequencies and powers, we can obtain the differential phase matrix (DPM) of tag-pair, with each element denoted by $\Delta\phi_{ij} = \left(\frac{4\pi\Delta d}{c} \times f_j + 2\Delta\alpha + \Delta\theta_{ij}\right) \bmod 2\pi$ where Δd is the differential tag-antenna distances, c is the speed of the electromagnetic wave, f_j is the j-th frequency, $\Delta\alpha$ is the differential tag-antenna intersection angle and $\Delta\theta_{ij}$ is the hardware fingerprint under i-th power and j-th frequency. Then, we unwrap the phase-frequency vector for each power based on the monotonicity. Every time we complete unwrapping a new phase-frequency vector, we compare it with the vector of the last power and conduct phase unwrapping between vectors based on the continuity.

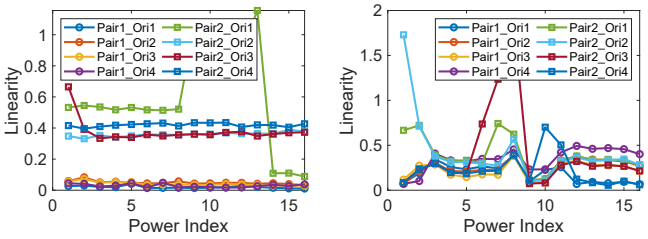
Fingerprint matching. The unwrapped DPM contains not only $\Delta\theta$ which we desire to extract, but also the distance factor Δd and orientation factor $\Delta\alpha$. Here we adopt the implicit method similar to [13] to match $\Delta\theta$. First, we subtract the registered $\Delta\tilde{\phi}_{ij}$ with the same EPCs (*i.e.*, IDs of tag-pair) from $\Delta\phi_{ij}$. Note that one DPM is collected beforehand and stored in the database as the registered one. For a legitimate tagged item, the theoretically subtracted result is $\frac{4\pi(\Delta d - \Delta\tilde{d})}{c} \times f_j$, which satisfies two properties:

- For any power, the result would linearly change with frequencies and the theoretical intercept of is zero (or integral multiple of 2π[1]).
- For any frequency, the result would not depend on the power changes.

Otherwise, for an illegitimate tagged item, the subtracted result $\Delta\phi_{ij} - \Delta\tilde{\phi}_{ij}$ would contain unmatched fingerprint terms $\Delta\theta_{ij} - \Delta\tilde{\theta}_{ij}$ under different frequencies and powers (i, j), which makes the above two properties do not hold, *i.e.*, low linearity across frequencies and instability across powers. Based on this observation, we then conduct zero-intercept linear regression on each phase-frequency vector $\Delta\phi_i - \Delta\tilde{\phi}_i$ for each power index:

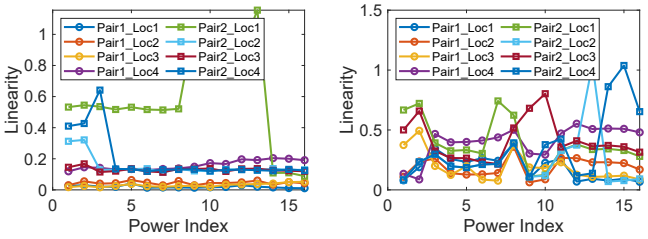
$$\kappa_i^* = \arg\min_{\kappa_i} \sum_{j=1}^{N} \left(\Delta\phi_{ij} - \Delta\tilde{\phi}_{ij} - \kappa_i \times f_j\right)^2, \forall i \quad (1)$$

[1]Within a certain distance range, there is only zero-intercept situation and this paper focuses on this situation.



(a) Antenna #1 (b) Antenna #2

Fig. 3: ICV vs. Orientations.



(a) Antenna #1 (b) Antenna #2

Fig. 4: ICV vs. Locations.

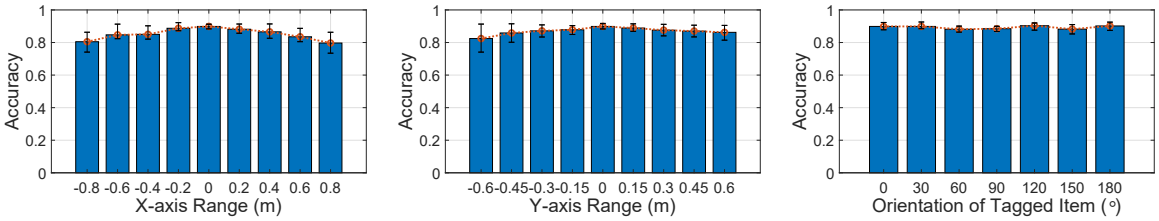
where κ_i is the phase vector's fitted slope of i-th power.

Next, to measure the linearity and judge the legitimacy, we calculate the standard deviation of fitting for each power:

$$\sigma_i = \sqrt{\frac{1}{N}\sum_{j=1}^{N}\left(\kappa_i^* \times f_j - \Delta\phi_{ij}^{A_2} + \Delta\tilde{\phi}_{ij}^{A_2}\right)^2}, \forall i \quad (2)$$

where $\boldsymbol{\sigma} = \{\sigma_1, \sigma_2, ..., \sigma_M\}$ is defined as inductive coupling-related vector (ICV), which indicates the fingerprint matching result. Here we only exploit the first property (*i.e.*, linearity across frequencies) and the usage of the second property (*i.e.*, stability across powers) will be explored in the future work.

To verify the resolution and robustness of ICV, we use one ImpinJ R420 reader [14], E9028PCRNF antennas and two pairs H47 tags for benchmark experiments (see Fig. 1). Fig. 3 and Fig. 4 demonstrate the ICVs under different item's orientation and locations, where $\Delta\tilde{\phi}_{ij}$ of Pair1 is used as registered one. From Fig. 3, we can find that for Antenna #1, the ICV of Pair2 (*i.e.*, the different tag-pair) reaches an extremely high value ($\|\boldsymbol{\sigma}\|_\infty = 1.156$) while that of Pair1 (*i.e.*, the same pair) is only 0.041, at the same location and orientation. Besides, the average value $\bar{\boldsymbol{\sigma}}$ of Pair2 is 29.78×



(a) Accuracy vs. X-axis movement (b) Accuracy vs. Y-axis movement (c) Accuracy vs. Orientations

Fig. 5: Authentication accuracy under different locations and orientations.

greater than that of Pair1. When the item's orientation angle changes to 45°, 90° and 135° respectively, the $\bar{\sigma}$ of Pair1 can still remain fairly small values (0.049, 0.041 and 0.029), which indicates the robustness of ICV to orientation changes. Also, the $\bar{\sigma}$ of Pair2 (0.359, 0.378 and 0.420) is evidently larger than that of Pair1, even under different orientations, though the gap is decreased a bit. This is probably because the extracted fingerprint after orientation changes may deviate from its original value and approach the other tag-pair's fingerprint. Meanwhile, the ICVs obtained from Antenna #2 are not distinguishable as those from Antenna #1 at many power indices, even though the $\|\boldsymbol{\sigma}\|_\infty$ of Pair2 is still large. This is reasonable since the collected phases of Antenna #2 (and Antenna #3 as well) would be affected by environmental multipaths more easily than those of Antenna #1 due to the deployment-related polarization difference [15]. So the deployment way of Antenna #1 is preferred and adopted in the subsequent evaluation part (Section III). Similarly, when the item's location changes, the gap of $\bar{\sigma}$ between Pair1 and Pair2 also exists, whereas $\bar{\sigma}$ may reach a relatively high value at some remote location (see Fig. 4). This reveals that the effective authentication range is extended but still finite. In conclusion, the above experimental result shows that the extracted ICV is robust to orientation and a certain range of location changes.

Tagged item validation. After we obtain the ICV of the tag-pair, we input it into a threshold-based classifier where $\bar{\sigma}$ is used to validate the genuineness of tag-pair. The value of threshold is trained in advance to achieve the maximum classification accuracy. Note that the other classifiers can be used as well and here we just set a threshold for simplicity.

III. Evaluation

A. Experimental Setup

We randomly attach 100 tag-pairs on the items and conduct evaluations in the same environment as Fig. 1. The reader configurations and phase collection is implemented through LLRP [16]. Here the ranges of transmission power and frequency channels we use are 26.0∼30.0 dBm and 920.625 ∼924.375 MHz. The system and corresponding algorithms are developed in Java and MATLAB languages.

For each tag-pair, we compare its DPM with the registered DPMs of all tag-pairs and the extracted ICVs contain a valid one and 99 invalid ones. In this way, we collect 50 sets of ICVs for each tag-pair under each location or orientation, and can obtain a dataset of ICVs with labels, where 70% of them are used for training and 30% of them are used for testing. Besides the authentication performance under different settings, our evaluations on FreeAuth also contain the measurement and comparison of effective authentication range with SOTA methods.

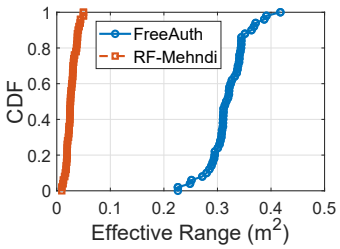


Fig. 6: Comparison of effective authentication range

B. Authentication Performance

Robustness to Location. We define the projection point of Antenna #1 as the origin and then evaluate the authentication accuracy on each point along X-axis and Y-axis, with intervals of 10cm and 15cm respectively. Fig. 5(a) and Fig. 5(b) show the accuracy results at different locations. It can be found that in the range of $|x| < 0.8$m and $|y| \leq 0.6$m, FreeAuth can maintain good authentication accuracy (at least 80%). Among all locations, the closer the location is to the origin, the higher the authentication accuracy is. Also, the authentication accuracy at the edge location is relatively lower. For example, the accuracy at the position x = -0.8cm is 80.48% and that at the position y = -0.6cm is 82.43%, whereas the accuracy rate at the origin can reach 89.87%. This conforms to our intuition because the ICV extracted in adjacent places will be relatively closer. In addition, we can find that the accuracy of the symmetrical position of the X-axis or Y-axis direction is very close. This is reasonable because the radiation beam of the reader antenna is spatially symmetric in theory. In summary, although the location (distance) factor exerts some influence on the fingerprint matching results, the performance of our method does not depend on the locations in a certain range.

Robustness to Orientation. Similar to the location factor, we adjust the item's 2D orientation angle to 0° ∼180° with the step of 30°. From the Fig. 5(c), we can see that FreeAuth maintains a fairly high accuracy (over 88.15%) regardless of the orientation changes and the accuracy gap between different orientations is less than 2.61%. The results confirm that our method can effectively eliminate the interference of

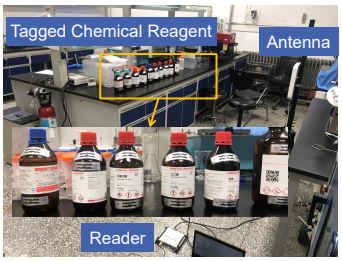


Fig. 7: Case study in the chemical lab

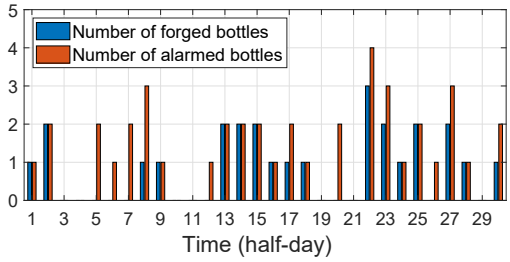


Fig. 8: Result of chemical reagent anti-counterfeiting

the polarization effect on DPM. Besides, we surprisingly find that the accuracy would even increase when rotating to some angles (*e.g.*, 120°), probably due to the diverse multipath effect under different orientations. Moreover, actually when the item's orientation changes, the distance factor also changes by a small degree (<0.1m). Despite this, we have proven that FreeAuth is robust to distance changes in a small range and this would not affect the evaluation results regarding the orientation factor.

Effective authentication range. Based on the symmetry, we put the item on the edge positions and calculate the accuracy at these positions to find the farthest position supporting ≥80% accuracy. As shown in Fig. 6, compared with the SOTA method RF-Mehndi [5], our method FreeAuth can support larger effective authentication area by 11.67×, which achieves 0.32m^2 in average. This significantly demonstrates the effectiveness of FreeAuth to enhance the robustness to location changes. Note that due to the low resolution of TagPrint [4] and workflow incompatibility of EingerPrint [6], we only compare FreeAuth with RF-Mehndi here.

C. Case Study

We study the practical effect of FreeAuth in the anti-counterfeiting system for chemical reagents as shown in Fig. 7, where three volunteers are arranged to play the role of attackers to substitute forged reagent bottles for the genuine ones randomly during 15 days. The replaced reagent bottle is attached by the tag-pair with the same EPC as the original reagent bottle. Fig. 8 shows the number of alarmed reagent bottles detected by the FreeAuth system every 12 hours. All forged reagent bottles (totally 26 bottles) are detected, and the remaining alarmed ones (16 bottles) include false detection of real reagents and some reagents transferred to other laboratories (accounting for 31.25% and 68.75% respectively). This result greatly indicates the practical utility of FreeAuth, without requiring any information about the attacker.

IV. Conclusion

In this work, we present an effective system FreeAuth to authenticate RFID tags accurately only with COTS devices, regardless of the tagged item's location and orientation changes. To achieve this, an implicit fingerprint matching algorithm is designed. We implement FreeAuth and the experimental results show a high authentication accuracy of 89.87% and also a large effective authentication range of around 0.32m^2. Moreover, the case study in the chemical lab verifies FreeAuth as a promising system for real-world deployment.

References

[1] A. Juels, "Rfid security and privacy: A research survey," *IEEE Journal on Selected Areas in Communications (JSAC)*, vol. 24, no. 2, pp. 381–394, 2006.

[2] Q. Pan, Z. An, X. Yang, X. Zhao, and L. Yang, "Rf-dna: large-scale physical-layer identifications of rfids via dual natural attributes," in *Proceedings of ACM Annual International Conference on Mobile Computing and Networking (MobiCom)*, 2022, pp. 419–431.

[3] J. Li, A. Li, D. Han, Y. Zhang, T. Li, and Y. Zhang, "Rcid: Fingerprinting passive rfid tags via wideband backscatter," in *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)*, 2022, pp. 700–709.

[4] L. Yang, P. Peng, F. Dang, C. Wang, X.-Y. Li, and Y. Liu, "Anti-counterfeiting via federated rfid tags' fingerprints and geometric relationships," in *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)*, 2015, pp. 1966–1974.

[5] C. Zhao, Z. Li, T. Liu, H. Ding, J. Han, W. Xi, and R. Gui, "Rf-mehndi: A fingertip profiled rf identifier," in *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)*, 2019, pp. 1513–1521.

[6] X. Chen, J. Liu, X. Wang, H. Liu, D. Jiang, and L. Chen, "Eingerprint: Robust energy-related fingerprinting for passive rfid tags," in *Proceedings of USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, 2020, pp. 1101–1113.

[7] Y. Zhu, C. Duan, X. Ding, and Z. Yang, "B-aut: A universal architecture for batch rfid tags authentication," in *Proceedings of the IEEE International Conference on Parallel and Distributed Systems (ICPADS)*. IEEE, 2021, pp. 755–762.

[8] J. Han, C. Qian, Y. Yang, G. Wang, H. Ding, X. Li, and K. Ren, "Butterfly: Environment-independent physical-layer authentication for passive RFID," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, vol. 2, no. 4, pp. 1–21, 2018.

[9] M. Piva, G. Maselli, and F. Restuccia, "The tags are alright: Robust large-scale RFID clone detection through federated data-augmented radio fingerprinting," in *Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, 2021, pp. 41–50.

[10] J. Han, C. Qian, P. Yang, D. Ma, Z. Jiang, W. Xi, and J. Zhao, "GenePrint: Generic and accurate physical-layer identification for UHF RFID tags," *IEEE/ACM Transactions on Networking (ToN)*, vol. 24, no. 2, pp. 846–858, 2015.

[11] D. M. Dobkin, *The RF in RFID: UHF RFID in practice*. Newnes, 2012.

[12] J. Wang, L. Chang, O. Abari, and S. Keshav, "Are RFID sensing systems ready for the real world?" in *Proceedings of the ACM Conference on Mobile Systems, Applications, and Services (MobiSys)*, 2019, pp. 366–377.

[13] Y. Zhu, C. Duan, X. Ding, and Z. Yang, "Readerprint: A universal method for rfid readers authentication based on impedance mismatch," in *Proceedings of Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, 2022, pp. 352–360.

[14] Impinj. Impinj inc. [Online]. Available: http://www.impinj.com

[15] Y. Zhu, C. Duan, X. Ding, and Z. Yang, "Rosense: Refining los signal phase for robust rfid sensing via spinning antenna," *IEEE Internet of Things Journal*, vol. 9, no. 23, pp. 24 135–24 147, 2022.

[16] E. EPCglobal, "Low level reader protocol (llrp)," 2010.